Cybersecurity Policy for a Sustainable Circular Bioeconomy: An Overview

Maria Lourdes Ordoñez Olivo

Hungarian University of Agriculture and Life science, Hungary,
Ordonez.Lourdes.Maria@phd.uni-mate.hu

Lourdes Ruiz Salvador

Obuda University, Budapest, Hungary, lourdes.ruiz@bgk.uni-obuda.hu

Abstract: A sustainable circular bioeconomy includes interconnected complex supply chains in which data is shared with various stakeholders such as manufacturers, farmers, and researchers. It also relies on sensitive data acquisition via IoT sensors, posing unique cybersecurity risks. This study offers an overview of the cybersecurity threat landscape in a sustainable circular bioeconomy. It assesses cybersecurity policies addressing the risks of interconnectedness, data sensitivity, operational technology vulnerabilities, and emergent technologies. It analyzes critical elements such as data governance, operational technology security, end-to-end supply chain data protection, incident response, recovery, training, and awareness. Furthermore, it proposes a holistic approach comprising the integration of sustainability initiatives into cybersecurity operations.

Keywords: circular, bioeconomy, sustainability, cybersecurity,

1 Introduction

The circular bioeconomy (CBE) has had various definitions during the last decade, with a common framework for sustainable bioeconomy and the achievement of SDGs. For the European Commission, in their "Circular Economy Action Plan", the CE is the economic space where the value of products, materials, and resources is maintained in the economy for as long as possible with a minimal waste generation [1]. To supplement this vision, the Ellen MacArthur Foundation describes the circular economy as keeping goods, components, and materials at their peak usability and worth at all times, distinguishing between technical and biological cycles [2].

The two concepts share a focus on the sustainable and efficient use of resources that produce the least amount of waste. These ideas are entirely consistent with the Sustainable Development Goals, which aim to balance countries' social, economic, and environmental progress and ensure that by 2030, all people live in peace and prosperity [3].

According to [4], bioeconomy businesses can considerably boost their competitiveness by incorporating innovative technologies and digitalization into their operations. The implementation of more efficient digital systems and other innovative technology shortens operational time, enhances product quality, attracts more customers, and expands into new markets faster.

Digitalization is closely related to the notions of industrial economic sectors, particularly the new industrial models known as Industry 4.0 and 5.0 because it reflects a considerable change in manufacturing and production processes caused by the integration of digital technologies[5]. In that regard, digitalization, globalization, and sustainability are three critical growth avenues for businesses today. Digitization can speed up data management, knowledge generation, and innovation processes, allowing for a more efficient and sustainable transition to production [6].

CBE represents a transformative sector that relies its efficiency and productivity on digitalization and interconnectedness. However, it introduces significant cyber risks and vulnerabilities to critical infrastructure, including bio-refineries, smart agriculture, and supply chain managing systems. Also, cybersecurity involving CBE is a pressing issue that lacks specific frameworks. The interconnectedness within CBE systems stimulates innovation and sustainability but expands the attack surface for malicious actors, potentially leading to disruptions in production, data breaches, and economic losses.

This review article delves into the relationship between cybersecurity policy and sustainable CBE, focusing on the evolving threat landscape, international cybersecurity frameworks tailored to CBE, and best practices. This paper will add to the discussion of secure digital transformation in sustainability-driven economies, assisting researchers in creating strong cybersecurity measures for a resilient circular bioeconomy.

2 Overview

2.1 Circular Bioeconomy and Its Digital Transformation

According to [7], the circular economy is based on five guiding principles: a) regeneration of ecosystems; b) minimization of waste and avoiding non-essential products; c) prioritizing biomass flows for basic human needs; d) using and recycling ecosystem by-products; and finally, e) using renewable energies while minimizing total energy use.

The circular bioeconomy requires an integrative perspective, as biomass is produced and used by many economic sectors, such as agriculture, manufacturing industries, energy, and pharmaceuticals.

Digital transformation in industrial sectors is an essential enabler of the circular economy because it allows for the collection and analysis of data related to assets and processes, which improves decision-making and optimizes processes by generating more significant flows of data and digital information [8]. Furthermore, it allows for the analysis of vast amounts of data on resource consumption, product performance, and waste generation, making it easier for businesses to identify possibilities to cut and reuse resources [9].

McKinsey and HBR conducted research to assess digital maturity in 22 industries, focusing on criteria such as digital spending, business processes, work digitization, digital asset stock, transactions, etc. As a result, information technology tops all industries, followed by media, banking and insurance, and professional services. These four industries have created a digital enablement culture that encourages end-user acceptance and usage, broadens their offers, enables self-service, and more. According to the survey, the public and government, healthcare, hotel, construction, and agriculture sectors are the top five laggards in terms of digital adoption initiatives and programs. The gap in digitization in healthcare and agriculture is due to the highly regulated nature of both sectors [10]. Agriculture and hunting, according to the same survey, have the lowest digitization scores across all categories and criteria (Figure 1). Over the last two decades, automatic guidance has been used on more than half of the land planted by maize, cotton, rice, sorghum, soybean, and winter wheat. By 2024, 85% of US farmers will have used at least one precision farming technique, such as GPS or remote sensing(Olmstead, 2024).

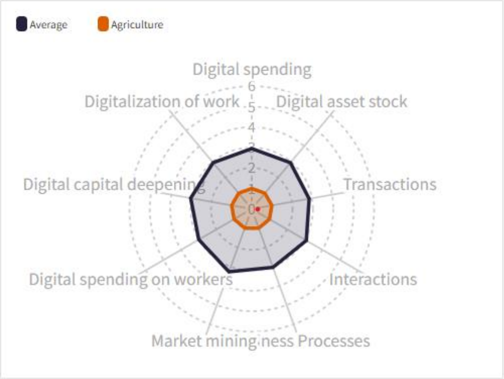

Figure 1.
Digital Transformation of the US Agriculture Sector[10]

According to the same research, digital transformation refers to how technology is altering the way manufacturing organizations function by automating administrative operations, providing better customer experiences, and increasing overall productivity. Manufacturing digitization encompasses RPA, 3D printing, knowledge work automation, predictive analytics for forecasting, mobile apps for frontline staff management, ERPs, RFID tracking, and more. Figure 2 illustrates the average digital adoption rate, calculated based on a digitization score of 3.75. According to Foundry's Digital Business Study, 89% of all manufacturing organizations have embraced a digital-first business model or plan to pursue digital transformation activities in the near future [10].

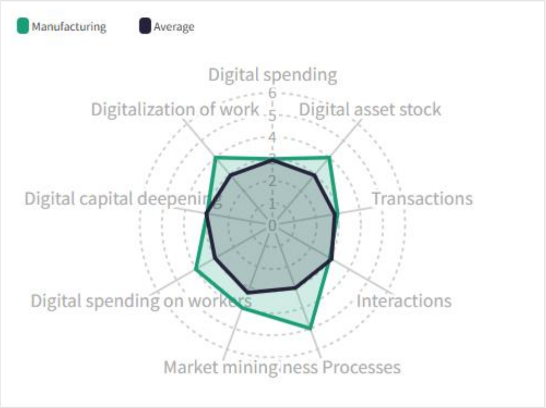

Figure 2.
Digital Transformation of the US Manufacturing Sector[10]

For example, in the agri-food sector, digitization can improve operations without requiring additional infrastructure, thanks to automated production and smart manufacturing technologies that enhance production efficiency and reduce resource consumption. One such current digital technology that permits remote device connectivity in agriculture has resulted in smart agriculture and precision farming, which are replacing conventional practices and promoting sustainable development [11]. The findings of the study of [12] in industrial organizations revealed that larger companies and those with a higher level of product innovation are more likely to achieve higher degrees of digital transformation. The research showed that digital transformation presents challenges for small and medium-sized businesses.

2.2 Digitalization in the Bioeconomy

Digitalization as a process is closely related to the notions of Industry 4.0 and 5.0 since it signifies a dramatic shift in manufacturing and production processes brought about by the integration of digital technologies. According to various studies, advanced digital technologies, such as digital applications, geospatial technologies, immersive environments, open and crowd-based platforms, proximity, blockchain, AI, Internet of Things (IoT), informatics, robotics, and 3D printing, among others, support the sustainable optimization process known as "sustainable business practices" in certain industries [13]. For instance, digital technologies make it easier to monitor environmental footprints, offering measurable data for sustainability indicators and encouraging innovation in product development and supply chain management [14].

The study by [15] determines which technologies are most extensively employed in industrial systems to fulfill particular SDGs. AI and geospatial technologies, for example, can be easily adapted to different business functions and processes to improve sustainable development; geospatial technology, in particular, collects critical environmental data for decision-making on energy resource management, climate change, and air and water quality. In addition, GPS can assist decision-makers in making better traffic management decisions and improving precision agriculture.

Regarding blockchain, although it is a relatively new (2008) technology, its implementation is spreading in production systems [13]The blockchain can help with transparency, traceability, and efficient resource management by improving corporate social responsibility and ensuring transparency and fairness in contract and payroll management, as well as tracing product life cycles, improving supply chain transparency, and encouraging responsible consumption. It can also monitor greenhouse gas emissions, encouraging the transition to a low-carbon economy[16].

2.3 Cybersecurity Risks in the Circular Bioeconomy

Digitally connected global enterprises benefit from numerous new opportunities, but business executives must not overlook the associated risks. According to [5] research, risks in the bioeconomy industry can be divided into five categories: a) security risks, b) technology risks, c) social risks such as professional obstacles for entrepreneurs and employees using digital tools, d) client capabilities in using digital tools, and e) additional hazards.

2.3.1 Risks related to IoT devices, smart agriculture, and bioinformatics.

For example, cybersecurity risks influence the rapid evolution of Information and Communication Technologies (ICT) in modern agriculture. Potential attacks on various intelligent agricultural systems can lead to serious security issues in the dynamic and distributed cyber-physical environment. These threats are mainly related to cybersecurity, data integrity, data loss, and online disconnection of heavy machinery connected online, among others [17]. A cyber-attack on an agricultural or food company is more feasible, as digitalization and the use of many devices connected to the Internet provide more opportunities for potential (cyber)criminals in areas that were previously too difficult to attack or too far away to approach physically [18].

Other examples are bioinformatics initiatives, which frequently require complicated and interdisciplinary tasks such as data gathering, processing, analysis, interpretation, and visualization. These tasks can present a variety of risks and uncertainties, including data quality, dependability, validity, reproducibility, scalability, security, and ethical concerns.

In 2023, the agri-food business saw around 160 cyberattacks, making it the ninth most attacked globally, creating supply chain disruptions. This business is susceptible because it is just starting to digital, and many producers still use antiquated IT technologies to run their operations[19].

Some examples of recent cyber-attacks reported by [20] were:

- In 2023, Dole was the target of a sophisticated ransomware assault in which attackers gained access to the personnel data of about 3,900 US workers. Dole's operations were severely damaged, resulting in an estimated loss of $10.5 million.
- Mondelez, the corporate behemoth behind Oreos, experienced a data breach that was detected in February 2023, during which attackers targeted its law firm, Bryan Cave. This affected over 50,000 current and past employees, and the extent of the harm took months to assess.

3 Cybersecurity Threat Landscape in the Circular Bioeconomy

The digitalization of biological processes and the interconnected systems within the circular bioeconomy network increases the attack surface and creates new vulnerabilities. Hence, integrating cybersecurity and biosecurity is primordial to protect sensitive data, strengthen sustainability efforts, and develop effective cybersecurity measures[21]. The following sections describe some of the principal threat vectors in CBE

3.1 Industrial Vulnerabilities

Industries within CBE, such as biomanufacturing and bioprocessing, depend on automation, IoT, AI, and cloud computing for production processes, which increase the number of cyber threats. Inadequate segmentation between IT and operational technology (OT) networks can allow attackers to infiltrate OT critical systems.

Moreover, the OT environment was isolated from IT networks, but using real-time data sensors to increase efficiency and connectivity gives cyber criminals access to OT environments that are not appropriately secured. As a result, IoT sensors and devices bring vulnerabilities to smart biomanufacturing. They possess weak encryption and default passwords, which give hackers easy access to exploit these connections[22], [23].

Additionally, AI-driven bioprocesses are vulnerable to AI training data poisoning, which can contaminate and affect production[24]. OT systems, such as Industrial Control Systems (ICS) and Supervisory Control and Data Acquisition (SCADA) systems, are widely used in bioprocessing plants. Using legacy software and hardware with known security flaws, remote ICS access, ICS-targeted malware, and zero-day vulnerabilities constitute major threats to the systems[25], [26]. Also, denial-of-service attacks and rogue firmware updates on bioreactors controlled by PLCs can disrupt the systems, causing product contamination and financial losses[27].

3.2 Supply Chain Vulnerabilities

CBE depends on global supply chains comprised of different stakeholders in processes such as raw material sourcing, manufacturing, distribution, logistics, and waste management, which adds entry points for cyberattacks. Malicious actors can infiltrate at any stage of the supply chain, disrupting the operations[28]. Additionally, the dependence of third-party vendors on software, hardware, data storage and processing, logistics, and transportation constitute critical vulnerabilities that create backdoors for cyber criminals[29].

Blockchain and Enterprise Resource Planning (ERP) are used for raw material traceability and logistics management. Blockchain records and data manipulation attacks can introduce contaminated or counterfeit materials into production processes. Thus, it can compromise the supply chain's traceability and reliability, affecting the quality of the products and customer trust[30].

3.3 Data Vulnerabilities

Bioeconomy industries collect, process, manage, and store highly sensitive data such as biological, proprietary bioprocesses, protocols, intellectual property (IP) related to clinical trials, pharmaceutical development, and bioengineering, which are high-value targets for attackers[31], [32]. IP theft and misuse of bioinformatics data can lead to bioweapon production and manipulation of critical biological systems, which pose significant security threats. Moreover, data breaches within circular systems are a rising issue involving privacy, ethical usage, and regulatory non-compliance, which can lead to legal consequences and financial penalties.

3.4 Ransomware and Cyber Espionage

Ransomware is an evolving threat across CBE. Food and agricultural sectors are the most vulnerable to these attacks, which leads to a cascading effect that impacts time-sensitive operations such as planting and harvesting, which can cause food shortages and economic losses [33]. Bio-based manufacturing, primarily pharmaceuticals, is a critical target affecting healthcare industries. These attacks alter control systems in biorefineries, waste management, and renewable energy infrastructures, compromising environmental safety [34], [35].

The development and innovation of sustainable technologies are the basis of CBE. Hence, IP theft and marketing intelligence regarding novel biomanufacturing processes, renewable energy techniques, sustainable agriculture, and strategic plans constitute valuable assets for technological and economic advantage. Cyber espionage involves different actors such as competitor companies, nations with strategic interests in bio economies, and industrial espionage groups. It significantly impacts innovative initiatives within organizations, giving an unfair advantage to competitors and hindering growth and sustainable practices[36].

4 Recommended Countermeasures and Best Practices

Risks and threats are constantly emerging within CBE. Therefore, a multi-layered security approach is the most suitable option for safeguarding innovation, research, and sustainability actions. In addition, various strategies are presented below:

1. Cyber biosecurity is an emerging field that lacks specific cybersecurity policy frameworks. In this context, current cybersecurity policies must be adapted to this field. ICS and SCADA networks used in biomanufacturing processes require adopting these guidelines to strengthen security levels. Table 1 lists international frameworks and their relevance to circular bioeconomy.

Framework	Description	Relevance	Reference
National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF)	Comprehensive guidelines for cybersecurity risk management for protecting critical infrastructure. It focuses on five aspects: Identify, Protect, Detect, Respond, and Recover.	It applies to bio-industrial facilities such as biomanufacturing and biorefineries.	[37]
ISO 27001	International standards for information security management systems	It protects bio-based data, including genomic, biorepositories, and biotechnology research.	[38]
General Data Protection Regulation (GDPR)	European Union's personal data privacy and security regulations	It protects genomic data privacy and ensures compliance of biotech industries.	[39]
Cybersecurity & Infrastructure Security Agency's (CISA) ICS security guidelines	Offers directions to protect ICS environments	It secures automated processes in different industries, such as biomanufacturing and precision agriculture.	[40]
SANS Institute's OT Cybersecurity Critical Control	It comprises five critical ICS controls: Incident Response, Defensive Architecture, Network visibility monitoring, Secure Remote Access, and Risk-Based Vulnerability Management.	It provides specific guidelines regarding OT, which is widely used in circular bioeconomy.	[41]

Table1.
International cybersecurity framework and circular bioeconomy relevance

2. General cybersecurity practices are fundamental for enhancing a secure posture. These practices include strong password implementation, multifactor authentication (MFA), updating software and firmware, network segmentation, secure data backups and storage, comprehensive cybersecurity training to staff, developing and implementing incident response plans, regular security audits, penetration testing, and vulnerability assessments.

3. Specific cybersecurity practices addressing the challenges in circular bioeconomy include[42], [43], [44]:
    - Cybersecurity policies for AI include AI-driven bioengineering operations, ethical AI governance, and AI accountability policies.
    - Zero-trust architecture implementation in digital biomanufacturing platforms to protect IP and genetic databases
    - Intrusion Detection Systems (IDS) implementation for cyber threats monitoring in smart biomanufacturing facilities.
    - Blockchain and ERP systems protection via quantum-resistant cryptography and MFA.
    - Supply chain cybersecurity: Blockchain-based traceability for resource sourcing and IoT security, including device authentication and end-to-end encryption for data flow.
    - Data protection via encryption, anonymization techniques
    - Cyber Threat Intelligence, including AI-based analysis for threat detection.

Conclusions

This document discusses the cybersecurity threat landscape within the sustainable circular bioeconomy (CBE). It highlights that CBE involves complex, interconnected supply chains and relies on sensitive data acquired through IoT sensors, which creates unique cybersecurity risks. This study emphasizes the importance of addressing these risks through robust cybersecurity policies and practices. It also proposes a holistic approach that integrates sustainability initiatives into cybersecurity operations. Additionally, international cybersecurity standards and regulations provide a solid baseline to address risks and vulnerabilities in circular bioeconomy. However, it is encouraged that a tailored security guideline be developed, considering its unique characteristics. Cybersecurity awareness is key between the main actors in each circular bioeconomy sector. Policymakers, businesses, and researchers are required to develop and implement cybersecurity national-level strategies addressing the principles of the CBE.

References

[1] M. Carus and L. Dammer, 'The Circular Bioeconomy—Concepts, Opportunities, and Limitations', Industrial Biotechnology, 14, Apr. 2018, doi: 10.1089/ind.2018.29121.mca.

[2] Ellen Macarthur Foundation, 'Towards a circular economy: Business rationale for an accelerated transition', Dec. 2015. Accessed: Mar. 28, 2025. [Online]. Available: https://www.ellenmacarthurfoundation.org/towards-a-circular-economy-business-rationale-for-an-accelerated-transition

[3] United Nations, 'THE 17 GOALS | Sustainable Development'. Accessed: Mar. 28, 2025. [Online]. Available: https://sdgs.un.org/goals

[4] A. Miceikienė, 'The role of digitalization in the development of bioeconomy businesses', Baltic Rim Economies, 2022. Accessed: Mar. 28, 2025. [Online]. Available: https://sites.utu.fi/bre/the-role-of-digitalization-in-the-development-of-bioeconomy-businesses/

[5] S. Zeverte-Rivza, I. Brence, I. Gudele, B. Rivza, and P. Rivza, 'Digitalization Risks in the Bioeconomy: An Enterprise-Level Perspective', Sustainability, 16(2), Art. no. 2, Jan. 2024, doi: 10.3390/su16020524.

[6] M. Rennings, A. P. F. Burgsmüller, and S. Bröring, 'Convergence towards a digitalized bioeconomy—Exploring cross-industry merger and acquisition activities between the bioeconomy and the digital economy', Business Strategy & Development, 6(1), pp. 53–74, 2023, doi: 10.1002/bsd2.223.

[7] A. Muscat et al., 'Principles, drivers and opportunities of a circular bioeconomy', Nat Food, 2(8), pp. 561–566, Aug. 2021, doi: 10.1038/s43016-021-00340-7.

[8] C. Chauhan, V. Parida, and A. Dhir, 'Linking circular economy and digitalisation technologies: A systematic literature review of past achievements and future promises', Technological Forecasting and Social Change, 177, p. 121508, Apr. 2022, doi: 10.1016/j.techfore.2022.121508.

[9] K.-P. Lin, C.-M. Yu, and K.-S. Chen, 'Production data analysis system using novel process capability indices-based circular economy', Industrial Management &amp; Data Systems, 119(8), pp. 1655–1668, Aug. 2019, doi: 10.1108/IMDS-03-2019-0166.

[10] L. Olmstead, 'Digital Transformation & Tech Adoption by Sector (2025) - Whatfix', The Whatfix Blog | Drive Digital Adoption. Accessed: Mar. 28, 2025. [Online]. Available: https://whatfix.com/blog/digital-transformation-by-sector/

[11] B. Bisht et al., 'Industry 4.0 Digital Transformation: Shaping the Future of Food Quality', Food Control, vol. 170, p. 111030, Nov. 2024, doi: 10.1016/j.foodcont.2024.111030.

[12] C.-H. Wu, C.-W. Chou, C.-F. Chien, and Y.-S. Lin, 'Digital transformation in manufacturing industries: Effects of firm size, product innovation, and production type', Technological Forecasting and Social Change, vol. 207, no. C, 2024, Accessed: Mar. 28, 2025. [Online]. Available: https://ideas.repec.org//a/eee/tefoso/v207y2024ics0040162524004220.html

[13] V. Varriale, M. A. Camilleri, A. Cammarano, F. Michelino, J. Müller, and S. Strazzullo, 'Unleashing digital transformation to achieve the sustainable development goals across multiple sectors', Sustainable Development, 33(1), pp. 565–579, 2025, doi: 10.1002/sd.3139.

[14] W. Vanhaverbeke, 'What is the Impact of Digital Technologies on Reaching Sustainability Goals at the Company Level?', Linkedin. Accessed: Mar. 28, 2025. [Online]. Available: https://www.linkedin.com/pulse/what-impact-digital-technologies-reaching-goals-level-vanhaverbeke-3dope/

[15] V. Varriale, A. Cammarano, F. Michelino, and M. Caputo, 'The role of digital technologies in production systems for achieving sustainable development goals', Sustainable Production and Consumption, vol. 47, pp. 87–104, Jun. 2024, doi: 10.1016/j.spc.2024.03.035.

[16] M. Dionisio, S. J. de Souza Junior, F. Paula, and P. C. Pellanda, 'The role of digital social innovations to address SDGs: A systematic review', Environ Dev Sustain, vol. 26, no. 3, pp. 5709–5734, Mar. 2024, doi: 10.1007/s10668-023-03038-x.

[17] K. Demestichas, N. Peppes, and T. Alexakis, 'Survey on Security Threats in Agricultural IoT and Smart Farming', Sensors, 20(22), Art. no. 22, Jan. 2020, doi: 10.3390/s20226458.

[18] L. Barreto and A. Amaral, 'Smart Farming: Cyber Security Challenges', in 2018 International Conference on Intelligent Systems (IS), Sep. 2018, pp. 870–876. doi: 10.1109/IS.2018.8710531.

[19] Biotechnology, 'What is the best way to manage risks and uncertainties in a bioinformatics project?', Linkedin. Accessed: Mar. 28, 2025. [Online]. Available: https://www.linkedin.com/advice/1/what-best-way-manage-risks-uncertainties-bioinformatics

[20] Wanda, 'Understanding Cyber Threats in the Food Manufacturing Industry', TXOne Networks. Accessed: Mar. 28, 2025. [Online]. Available: https://www.txone.com/blog/understanding-cyber-threats-in-food-manufacturing-industry/

[21] M. Elgabry and S. Johnson, 'Cyber-biological convergence: a systematic review and future outlook', Front Bioeng Biotechnol, 12, p. 1456354, Sep. 2024, doi: 10.3389/fbioe.2024.1456354.

[22] P. Pal et al., 'Circular Bioeconomy in Action: Transforming Food Wastes into Renewable Food Resources', Foods, 13(18), Art. no. 18, Jan. 2024, doi: 10.3390/foods13183007.

[23] Omorinsola Bibire Seyi- Lande et al., 'Circular economy and cybersecurity: Safeguarding information and resources in sustainable business models', Financ. account. res. j., 6(6), pp. 953–977, Jun. 2024, doi: 10.51594/farj.v6i6.1214.

[24] O. Adeyeye, I. Akanbi, I. Emeteveke, and O. Emehin, 'Leveraging Secured Ai-Driven Data Analytics For Cybersecurity: Safeguarding Information And Enhancing Threat Detection', International Journal of Research Publication and Reviews, vol. 5, pp. 3208–3223, Oct. 2024, doi: 10.55248/gengpi.5.1024.2911.

[25] Legit Security, 'What's a Zero-Day Vulnerability? Prevent Exploits and Attacks'. Accessed: Mar. 18, 2025. [Online]. Available: https://www.legitsecurity.com/blog/what-is-zero-day-vulnerability

[26] K. Stouffer, S. Lightman, V. Pillitteri, M. Abrams, and A. Hahn, 'Guide to Industrial Control Systems (ICS) Security', National Institute of Standards and Technology, NIST Special Publication (SP) 800-82 Rev. 2 (Withdrawn), Jun. 2015. doi: 10.6028/NIST.SP.800-82r2.

[27] S. Goswami, S. Sarkar, K. Gupta, and S. Mondal, 'The role of cyber security in advancing sustainable digitalization: Opportunities and challenges', Journal of Decision Analytics and Intelligent Computing, 3, pp. 270–285, Dec. 2023, doi: 10.31181/jdaic10018122023g.

[28] Cloud Range, 'Current Cyber Threats in OT/ICS: What You Need to Know', Cloud Range. Accessed: Mar. 26, 2025. [Online]. Available: https://www.cloudrangecyber.com/news/current-cyber-threats-in-otics-what-you-need-to-know

[29] L. Ruiz Salvador, B. Fregan, and Z. Rajnai, 'ICT and Telecommunications Supply Chain: Threat Landscape and Countermeasures', in 2024 IEEE 11th International Conference on Computational Cybernetics and Cyber-Medical Systems (ICCC), Apr. 2024, pp. 1–6. doi: 10.1109/ICCC62278.2024.10582943.

[30] H. Fang, F. Fang, Q. Hu, and Y. Wan, 'Supply Chain Management: A Review and Bibliometric Analysis', Processes, vol. 10, p. 1681, Aug. 2022, doi: 10.3390/pr10091681.

[31] D. Rathnayake, 'Cyberbiosecurity: Where Digital Threats Meet Biological Systems | Tripwire', Tripwire Integrity Management. Accessed: Mar. 21, 2025. [Online]. Available: https://www.tripwire.com/state-of-security/cyberbiosecurity-where-digital-threats-meet-biological-systems

[32] E. National Academies of Sciences et al., ‘ECONOMIC AND NATIONAL SECURITY RISKS PERTAINING TO THE BIOECONOMY’, in Safeguarding the Bioeconomy, National Academies Press (US), 2020. Accessed: Mar. 21, 2025. [Online]. Available: https://www.ncbi.nlm.nih.gov/books/NBK556435/

[33] J. Marston, ‘Ransomware attacks on food and ag expected to rise, possible “cascading impacts” on the sector’, AgFunderNews. Accessed: Mar. 26, 2025. [Online]. Available: https://agfundernews.com/ransomware-attacks-on-food-and-ag-expected-to-rise-with-cascading-impacts-on-the-sector

[34] Lawrence, ‘Closing the cybersecurity gap: the hidden threat to renewables’, Energy Monitor. Accessed: Mar. 26, 2025. [Online]. Available: https://www.energymonitor.ai/sponsored/closing-the-cybersecurity-gap-the-hidden-threat-to-renewables/

[35] A. Roy, ‘Analyzing the Sunpharma Ransomware Attack: Implications for Cybersecurity Laws, Regulations, and Guidelines in the Pharmaceutical Industry’, IJISR, 14(1), pp. 1085–1092, Jun. 2024, doi: 10.20533/ijisr.2042.4639.2024.0123.

[36] B. Miller, ‘What is Corporate Espionage & How to Prevent It’, Mimecast. Accessed: Mar. 26, 2025. [Online]. Available: https://www.mimecast.com/blog/what-is-corporate-espionage-and-prevention-techniques/

[37] National Institute of Standards and Technology, ‘The NIST Cybersecurity Framework (CSF) 2.0’, National Institute of Standards and Technology, Gaithersburg, MD, NIST CSWP 29, Feb. 2024. doi: 10.6028/NIST.CSWP.29.

[38] L. Carter, ‘Circularity for Secure and Sustainable Products and Materials: A Draft Strategic Framework’, US Department of Energy, Oct. 2024. [Online]. Available: https://www.energy.gov/sites/default/files/2024-10/circularity-for-secure-sustainable-products-materials-report.pdf

[39] M. Nadeuau, ‘What is the GDPR, its requirements and facts?’, CSO United States. Accessed: Jun. 04, 2021. [Online]. Available: https://www.csoonline.com/article/3202771/general-data-protection-regulation-gdpr-requirements-deadlines-and-facts.html

[40] CISA, ‘Industrial Control Systems’, Cybersecurity and Infrastructure Security Agency CISA. Accessed: Mar. 27, 2025. [Online]. Available: https://www.cisa.gov/topics/industrial-control-systems

[41] R. Lee M. and T. Conway, ‘The Five ICS Cybersecurity Critical Controls’. SANS Institute, Oct. 2022. Accessed: Mar. 27, 2025. [Online]. Available: https://sansorg.egnyte.com/dl/R0r9qGEhEe

[42] M. De Donder, ‘Cyber Reality Bites into U.S. Food Supply Chain: How to Protect Your Operation’, Pinion Global. Accessed: Mar. 28, 2025. [Online]. Available: https://www.pinionglobal.com/blog/increased-threats-to-food-supply-chain-how-to-protect-your-operation/

[43] C. Sherman, ‘7 Emerging Cybersecurity Trends in Agribusiness You Need to Be Aware Of - Tech Support’. Accessed: Mar. 28, 2025. [Online]. Available: https://techsupport.farm/7-emerging-cybersecurity-trends-in-agribusiness-you-need-to-be-aware-of/

[44] A. Nagy, Y. Wu, K. Takács-György, Z. Rajnai, and B. Fregan, ‘Glance at Quantum Innovations in Crop Pest and Disease Detection: Bridging Physics and Agriculture’, in 2025 IEEE 23rd World Symposium on Applied Machine Intelligence and Informatics (SAMI), Jan. 2025, pp. 000289–000292. doi: 10.1109/SAMI63904.2025.10883296.